What is claimed is:

1. In a network including a plurality of hosts and a plurality of routers for facilitating the transmission of packets, a system for determining the point of entry of a malicious packet into said network using a representation of said malicious packet, said system comprising:

an intrusion detection system for detecting entry of said malicious packet into said network; and

a source-path isolation server responsive to operation of said intrusion detection system, for isolating said malicious packet;

whereby said point of entry of said malicious packet is determined.

2. The system of claim 1 and wherein said source-path isolation server further comprises:

means for generating a query message containing identification information about said malicious packet; and

means for forwarding said query message to certain of said plurality of routers displaced one hop away from said server.

3. The system of claim 2 and wherein said certain of said plurality of routers comprises:

means for generating a hash value of said identification information;

means for establishing a bit map of hash values representative of those of said packets which are transmitted through said certain of said plurality of routers; and

means for comparing said hash value against said hash values.

4. The system of claim 3 and wherein said certain of said routers further comprises:

means responsive to operation of said comparing means determining no match between said hash value and said hash values, for notifying said server that said malicious packet was not transmitted through said certain of said routers; and

means responsive to operation of said comparing means determining a match between said hash value and at least one of said hash values for notifying said server that

said malicious packet was transmitted through said certain of said routers and for forwarding said query message to other of said plurality of routers displaced one hop from said certain of said plurality of routers;

whereby determination of said point of entry of said malicious packet is pursued on a hop-by-hop basis.

5. In a network carrying a plurality of packets at least one of said packets being a target packet, said network including at least one network component, a detection device and a server, a method for determining a point of entry of a target packet into said network, said method comprising:

at said server, receiving said target packet from said detection device;

sending a query message identifying said target packet to a first component of said at least one network component;

receiving a reply containing information about said target packet from said first component;

processing said reply to extract said information; and

using said information in a manner that said point of entry shall ultimately be determined.

6. The method of claim 5 and wherein said detection device is incorporated into said server.

7. The method of claim 5 and wherein said network further includes a host, said host including capability for placing packets onto said network.

8. The method of claim 5 and wherein said sending operates to include said target packet into said query message.

9. The method of claim 5 and wherein said query message comprises a representation of said target packet.

10. The method of claim 9 and wherein said representation is a hash of at least a portion of said target packet.

11. The method of claim 5 and wherein said one of said at least one network component is located one hop away from said server.

12. The method of claim 5 and wherein said one of said at least one network component is located more than one hop away from said server.

13. The method of claim 5 and wherein said first component forwards said reply to another of said at least one network component.

14. The method of claim 5 and wherein said first component is a router.

15. The method of claim 5 and wherein said information is hash information derived from hashing at least a portion of said query message to obtain a query hash value and using said query hash value to determine if said target packet has passed through said first component.

16. The method of claim 5 and wherein said determining is accomplished using a source path isolation technique.

17. The method of claim 16 and wherein said source path isolation technique includes a breadth-first search.

18. The method of claim 16 and wherein said source path isolation technique includes a depth-first search.

19. In a network carrying a plurality of packets, said plurality of packets including a target packet having entered through an intrusion location, a query packet, and a reply

packet generated in response to said query packet, said network including a network component having a first memory and a server having a second memory, said server comprising:

a bus communicatively coupled to said network;

said second memory communicatively coupled to said bus for storing data and machine-readable instructions; and

a processor communicatively coupled to said bus executing said machine-readable instructions for causing said server to place a query packet onto said network for transmission to said network component, said query packet being generated in response to detecting said target packet and further including information about said target packet, said processor further executing said machine-readable instructions to process said reply packet to identify said intrusion location.

20. The server of claim 19 and wherein detecting a target packet is accomplished by processing a notification packet received from said network.

21. The server of claim 19 and wherein said reply packet is generated in response to said network component comparing a first hash value of at least one of said plurality of packets to second hash value derived from at least a portion of said query packet.

22. The server of claim 21 and wherein said first hash value is stored in said first memory using a bit mapped array.

23. The server of claim 19 and wherein said reply packet is generated in response to said network component comparing a first representation of at least one of said plurality of packets to second representation derived from at least a portion of said query packet.

24. The server of claim 23 and wherein said first representation is stored in said first memory using a bit mapped array.

25. A communication medium for transporting data in a network, said network including a network component for generating a representation of an intruding packet, a server, and an intrusion detection device, said communication medium comprising:

media for carrying a query message comprising information about at least a portion of said intruding packet, said query message being created by said server in response to a triggering event indicating said intruding packet was detected by said intrusion detection device; and

media for carrying a reply generated by said network component in response to said query message, said network component matching said representation to said information in said query message and indicating a match therebetween;

whereby said match indicates said intruding packet has been encountered.

26. The communication medium of claim 25 and wherein said media for carrying a query message and said media for carrying a reply are a single media carrying said query message and said reply.

27. The communication medium of claim 25 and wherein said representation is a hash value.

28. In a network carrying a plurality of packets, a computer-readable data signal embodied in a transmission medium used to identify an intrusion location of a target packet, said network including a server and a network component having memory storing a like plurality of packet representations, each of said representations corresponding respectively to each one of said plurality of packets, said data signal comprising:

a header portion comprising an address of said network component; and

a body portion comprising at least a portion of said target packet, said body portion being compared to each of said packet representations wherein a match between said at least a portion of said target packet and one said packet representations indicates said network component encountered said target packet.

29. The data signal of claim 28 wherein said body portion further includes machine-readable instructions for causing said network component to modify its operation upon execution of said instructions.

30. In a network carrying a plurality of packets, said plurality of packets including a target packet having entered said network through an intrusion location, a computer-readable storage medium containing executable code for instructing a processor to generate a query in response to a triggering event, said network including a network component having memory storing representations of encountered packets, said executable code instructing said processor to perform operations comprising:

processing said triggering event to extract said first information about said target packet;

generating said query for placement onto said network, said query including second information about at least a portion of said target packet;

sending said query to said network component;

receiving a reply from said network component;

processing said reply; and

using said reply to facilitate identification of said intrusion location.

31. The computer-readable storage medium of claim 30 and wherein said reply is generated in response to comparing said second information to said representations.

32. The computer-readable storage medium of claim 30 and wherein said reply is generated only if said network component has observed said target packet.

33. The computer-readable storage medium of claim 30 and wherein said representations are generated by hashing at least one of said plurality of packets to produce a hash value and using said hash value as an index into said memory.

34. In a network carrying a plurality of packets, said network including a network component having memory storing first information about a subset of said plurality of

packets having passed through said network component and a processor for computing a first representation of a target packet and a second representation of a member of said subset of said plurality of packets, said memory for also storing second information about an intrusion location of said target packet in said network, said memory comprising:

a data structure stored in said memory, said data structure including information resident in a database used by a source path isolation program for determining said intrusion location, said data structure including:

a network component identification attribute corresponding to location of said network component;

a target packet attribute uniquely identifying said target packet; and

a reply packet attribute associated with all members of said subset including at least one of said member, said reply packet attribute being associated with said network component identification attribute to identify origin of said reply packet, said reply packet indicating said member was encountered if said first representation matches said second representation.